TRAFICOM
Liikenne- ja viestintävirasto

Finnish Transport and Communications Agency Traficom

Domain Name Registrar's Guide

Instructions and requirements for prospective .fi domain name registrars

Version 2.0 | June 2026

Version	Date	Description / change	Author
1.0	25 October 2018	Version 1 - original publication	Ari-Matti Husa
1.1	21 December 2018	Version 1.1	Ari-Matti Husa
1.2	6 September 2021	Updates to KATAKRI requirements (2.10.4)	Sami Salmen-suo
1.3	15 December 2023	Updates to the registrar's data protection obli-gations (2.7)	Mervi Malinen
1.4	19 January 2024	Update on restrictions for registrars outside the EU/EEA (2.7.1)	Mervi Malinen
1.5	18 January 2026	Updated pricing (1.1.1)	Sami Salmen-suo
1.6	17 February 2026	Added introduction; appendices A, B and C	Sami Salmen-suo
2.0	15 June 2026	Structural and visual improvements. Substan-tive additions and edits throughout all sections. Accessibility corrections.	Sami Salmen-suo

Note

This guide is an advisory document. The ultimate legal responsibility for the lawfulness of registrar activity rests at all times with the registrar itself.

Up-to-date legislation and Traficom's regulations are available at traficom.fi.

Table of Contents

Introduction

This guide is intended for everyone considering becoming a .fi domain name registrar with the Finnish Transport and Communications Agency Traficom, or who is already in the process of registering as one. It is equally useful for existing registrars who wish to refresh their knowledge of their obligations and the applicable requirements. The guide does not address the obligations of DNS service providers.

The guide covers two central areas:

- Chapter 1 - Tasks and obligations of the registrar: describes the registrar's statutory service obligations to customers, including registration, maintenance of information, renewal, cancellation and change of registrar.
- Chapter 2 - Information security in registrar activity: addresses requirements relating to information-security management, risk management, data protection, name servers and technical interfaces.

The content of this guide is based on the Act on Electronic Communications Services (917/2014) and on Traficom's Regulation 68 on domain names. The guide was last updated in June 2026 (version 2.0).

1 Tasks and obligations of the registrar

A domain name registrar assists and advises its customers on matters relating to .fi domain names. The registrar registers .fi domain names and carries out the changes requested by its customers.

The registrant of a domain name deals with their own registrar in all situations relating to .fi domain names. Under the Act on Electronic Communications Services (917/2014), the registrar has an obligation to ensure that the registrant's rights are realised.

At the request of their customers, registrars carry out the following actions for a .fi domain name:

- registration in Traficom's domain name register
- updating of details
- renewal of the registration period
- change of registrar
- transfer to another registrant
- cancellation.

In addition, the registrar is required to provide its customers with:

- general guidance relating to .fi domain names
- notification if the registrar's activity has ended or if Traficom has issued a prohibition decision concerning the registrar.

1.1 The registrar's service obligations and pricing

1.1.1 Payment for registration and renewal

The registrar pays Traficom for the registration and renewal of its customers' domain names through the registrar's technical interface. Registrations and renewals are deducted from the registrar's pre-payment account. Pricing is determined by the registration period:

Registration period	Price (incl. 0 % VAT)
1 year	**€12**
2 years	**€24**
3 years	**€36**
4 years	**€48**
5 years	**€60**

> ⚠ **Fees are not refunded**
>
> Traficom does not refund the fee to the registrar even where a domain name has been registered in error or where Traficom later removes the domain name from the register by decision.

1.2 Obligation to advise customers

The registrar must advise its customers before registering .fi domain names. Guidance must cover at least the form, content and lawfulness of the domain name.

This information must be available both to existing and prospective registrants of domain names, regardless of whether the customers have already entered into a contractual relationship with the registrar. Ultimate responsibility for the lawfulness of the domain name rests with the registrant.

The registrar must in addition make it clear how and from where the customer may, if they so wish, obtain the registrar transfer key or the domain name transfer key. It is sufficient that the customer is advised of this after they have entered into a contractual relationship with their registrar.

1.2.1 Minimum requirements for guidance

The registrar may decide how to fulfil its disclosure obligation, but in terms of content, the registrar must provide its customers with at least the following information concerning the content and form of the domain name:

Protected names and trademarks

Under the Act on Electronic Communications Services, the following names and marks are protected:

- names or marks entered in Finland's Trade Register, Trademark Register, Register of Associations, Register of Foundations or Register of Political Parties, the names of public bodies, state enterprises, independent public-law institutions, public-law associations and foreign-state diplomatic missions
- established names, secondary signs or trademarks within the meaning of the Trade Names Act and the Trademarks Act
- EU trademarks entered in the trademark register of the EUIPO
- designations of origin under the Food Act and indications referred to in the Act on geographical indications for craft and industrial products.

The registrar must provide its customers with links to the following registers:

- Finnish Patent and Registration Office (PRH): Business Information System, Register of Associations, Trademark Register - prh.fi
- European Union Intellectual Property Office (EUIPO): EU Trademark Register - euipo.europa.eu
- European Union register of geographical indications: eAmbrosia - ec.europa.eu/agriculture/eambrosia/geographical-indications-register

Lawfulness of the domain name

A domain name must not, at the time of registration:

- correspond to another party's protected name or mark, unless the registrant can present an acceptable ground for the registration
- resemble another party's protected name or mark, if the domain name is registered with an evident intent to derive benefit or cause harm.

Permissible characters in domain names

Permissible characters are the letters a-z, the digits 0-9, the national characters å, ä and ö, the characters of the Sami languages spoken in Finland, and the hyphen-minus.

National characters and ACE form (Punycode)

Domain names containing national characters are represented in the Domain Name System in ACE form (ASCII Compatible Encoding, Punycode).

Example: ääkkönen.fi → xn--kknen-fraa0m.fi

Customers must be informed of the technical limitations affecting domain names with national characters, and where appropriate should be advised to apply both for the name with the national characters and for an equivalent name without them (e.g. ääkkönen.fi and aakkonen.fi).

Conversion tools are available, for example, on Traficom's website.

Instructions for obtaining keys

The registrar must at all times offer its customers the opportunity to request a registrar transfer key or a domain name transfer key in writing. The registrar may, for example, set out the conditions and procedures for obtaining a key on its website.

1.3 Ensuring the accuracy and currency of information

The registrar shall keep its customers' details up to date in the .fi domain name register, both at the time of registration and thereafter as the details change. The registrar must identify its customers. The registrar must make publicly available the principles and procedures by which it ensures that the registrant details entered in the domain name register are accurate and up to date.

> **⚠ Critical obligation: registrant entry**
>
> A .fi domain name must always be registered in the name of its actual user. A domain name must not be registered in the name of a privacy or proxy service provider.
>
> The registrar must not enter a customer's domain name in its own name. An incorrect registrant entry may, in the worst case, give rise to liability for damages.

At the customer's request, the registrar must carry out the following changes:

- updating the registrant's contact details
- cancelling the domain name
- transferring the domain name to another registrant
- changing the registrar of the domain name
- renewing the domain name.

1.3.1 Updating contact details

The registrar must keep its .fi domain name customers' details up to date, both at the customer's request and on its own initiative. If the customer suffers loss as a result of the registrar's default, the customer may claim damages.

1.3.2 Statutory service address

Traficom uses the e-mail address recorded in the domain name register (the service address) for hearings and the service of documents. A document or decision sent to this address is deemed to have been served on the third day after the message is sent. The registrar must verify the technical functioning of the service address.

> **The importance of the service address**
>
> Notifying Traficom of the service address is mandatory both for the registrar itself and for each customer's domain name.
>
> It is the registrar's responsibility to provide the address and to keep it up to date.
>
> Additional e-mail addresses may also be entered in the system, for example for technical communication.

1.4 Renewing a domain name

A domain name entered in the domain name register is valid for a minimum of one year and a maximum of five years. The registrar may renew the entry for one, two, three, four or five years at a time.

1.4.1 The registrar's obligations as the registration period draws to an end

When the registration period of a .fi domain name is about to end, the registrar:

- notifies the registrant of the upcoming expiry in good time
- provides the registrant with instructions on how to make a renewal request
- explains to the registrant the consequences of failing to renew.

The registrar and the customer may agree on automatic renewal by contract. The supervision of contracts between the registrar and the registrant, and the resolution of any contractual disputes, fall outside Traficom's remit.

1.5 Cancelling a domain name

The registrant of a .fi domain name may, if they so wish, cancel their domain name before the end of its registration period. On request, the registrar removes the domain name from Traficom's register.

The registrar is responsible for ensuring that:

- a domain name is cancelled only at the request of the registrant or their authorised representative
- no outside party, intentionally or unintentionally, cancels domain names
- where the registrant is an organisation, the registrar verifies that the party requesting cancellation has the right to do so (for example a signing right entered in the trade register).

> **⚠ Problem situations relating to cancellation**
>
> The wrongful cancellation of a domain name may have significant financial consequences. In the worst case the registrar may incur liability for damages as a result of a wrongful cancellation.
>
> Questions of contract law, damages or consumer law arising from cancellation are resolved on the basis of other legislation.

1.6 Transferring a domain name to a new registrant

The registrant of a domain name may, if they so wish, transfer their valid domain name to another registrant. On receiving a transfer request, the registrar:

- verifies that the requester has the right to transfer the domain name
- sends the domain name transfer key to the registrant without seeing the content of the key code
- transfers the domain name from one registrant to another within five business days of the transfer key being delivered to the registrar.

> **Transfer key**
>
> The transfer key is a code defined by Traficom which the registrar neither sees nor sets.
>
> The key is always sent to the current registrant of the domain name, who must themselves provide it to the registrar for the transfer.
>
> The registrant may authorise either their own registrar or the receiving registrar to carry out the transfer. In the latter case, both the domain name transfer key and the registrar transfer key are required.

1.6.1 Right to submit a transfer request

The registrar must satisfy itself that no party other than the registrant of the domain name or their authorised representative is requesting the transfer. If the request is submitted by any other party, the requester must demonstrate sufficient authorisation.

1.6.2 Transfer time

The registrar must carry out the transfer technically within five business days from the time the former registrant has delivered the transfer key and the new registrant's details to the registrar. The time limit is a service-level requirement based on Traficom's regulation.

1.7 Changing the registrar

The registrant of a domain name is free to change their registrar. Changing the registrar does not require any particular reason.

Stages of the change

1. The registrant either authorises the new registrar to obtain the registrar transfer key from the former registrar or requests the key themselves from the former registrar and delivers it to the new registrar. The request must be made in writing.
2. The former registrar delivers the registrar transfer key within five business days of a legitimate request, once it has verified the requester's right to make the request.
3. The new registrar receives the transfer key and takes over administration of the domain name.

> **Registrar transfer key**
>
> A code by which the administration of a domain name is transferred from one registrar to another.
>
> The former registrar generates the key in the domain name register system and delivers it by its preferred means (for example by e-mail or telephone) to a legitimate requester.

1.7.1 Problem situations

If the former registrar does not deliver the transfer key to the new registrar or to the registrant within the time limit despite repeated requests, the new registrar may request that Traficom deliver the transfer key to the registrant.

1.8 When registrar activity ceases

The registrar must notify Traficom and its customers of the cessation of registrar activity and to the registrar's own customers at least two weeks in advance. This gives customers the opportunity to keep their domain names operational and to change the administrator of the name servers before the activity ends.

The notifications must be made to each customer individually. Communicating on the website alone is not sufficient. E-mail is an effective means, but it is advisable to seek to reach customers by telephone as well.

1.8.1 Notification of Traficom's prohibition decision

Traficom supervises the lawfulness of registrar activity and may issue a prohibition decision against a registrar where the registrar fails to remedy its default despite warnings.

If Traficom issues a prohibition decision, the registrar must notify its own customers without delay so that they can, if necessary, obtain a new registrar.

Traficom enforces the prohibition decision by closing the registrar's technical interface either so that the registrar can no longer register new domain names or, additionally, so that the registrar can no longer even maintain its existing domain names.

1.8.2 Closing the prepayment account

A registrar that has ceased its registrar activity may request Traficom to refund any unused balance held in its prepayment account.

1.9 Registering as a registrar

A party intending to become a .fi domain name registrar must, before notifying Traficom, familiarise themselves carefully with all the requirements laid down in Chapter 21 of the Act on Electronic Communications Services.

Registration as a registrar is carried out using Traficom's electronic form. Before the notification is approved, Traficom verifies that the registrar has completed the self-assessment tool defined by Traficom, which enables the registrar to demonstrate compliance with information-security obligations.

Changes to the registrar's details must be notified to Traficom without delay. Traficom recommends that updates be made within three days of any change.

The registrar may use the .fi registrar logo in its .fi domain name registrar activity. Versions of the logo suitable for publication are available on Traficom's website.

1.9.1 Reseller activity

Where the registrar makes use of resellers in its .fi domain name registrar activity, the registrar is also responsible for the resellers' conduct. The registrar must enter the details of the reseller in the .fi domain name register and keep them up to date. The registrar must record in the details of each domain name whether a reseller is used to administer that domain name.

2 Information security in registrar activity

The registrar must safeguard information security by preparing for threats and addressing any incidents. The minimum information-security requirements protect both the registrar activity and the rights of the domain name registrant.

Information security means, under section 3, point 28 of the Act on Electronic Communications Services, the administrative and technical measures taken to safeguard the confidentiality, integrity and availability of information.

The registrar must complete the information-security self-assessment tool specified by Traficom.

> **Documentation obligation**
>
> The contingency plan must be documented.
>
> Traficom's Regulation 68 on domain names sets out the minimum requirements for information-security management which the registrar must implement in its operations.
>
> On the basis of the documentation, Traficom can, where necessary, verify that the registrar is complying with its information-security obligations.

2.1 Information security in practice

The registrar must document and maintain an up-to-date description of how it addresses the various aspects of information security in its operations. Traficom does not separately specify the documents required - the overall documentation package is left to the registrar's own judgement.

2.1.1 Aspects of information security

The registrar must take the following aspects into account:

Administrative information security

- information-security governance documents (typically an information-security policy and architecture)
- processes and their management
- risk management and continuity assurance
- documentation practices and systems
- audit and exercise procedures.

Personnel security

- information-security responsibilities and duties of personnel
- information-security competence of personnel and its development
- background checks on personnel
- key-person risks
- prevention of dangerous combinations of responsibilities and duties, and job rotation
- procedures to be followed on termination of employment.

Hardware, software and communications security

- vulnerability management
- detection of information-security breaches
- change management.

Information-asset and operational security

- ensuring the confidentiality, integrity and availability of information
- classification of information assets and handling in accordance with the classification
- responsibilities for maintaining the access-rights register: granting, modifying and removing rights
- prevention of the accumulation of access rights
- prevention of unauthorised access to management and configuration information and to customer, billing and log data
- storage and destruction of information assets.

Physical security

- location of premises and the security of the surroundings
- access control
- structural protection.

Where necessary, Traficom is entitled to audit the registrar's activities as a domain name registrar.

2.2 Risk management

The registrar must identify the functions, information and systems that are important for the continuity of its registrar activity and must regularly assess and manage the information-security risks to which they are exposed. The processes and outcomes of risk management must be documented.

Information-security risks may arise, for example, from:

- human error
- shortcomings in, or non-observance of, instructions given to personnel
- theft or vandalism
- faults and malfunctions in equipment, systems or software

- the spread of malicious software
- the destruction of information assets
- fire or water damage
- errors and defaults by a subcontractor or by an operator in the partnership network.

Objectives of risk management

The objectives of risk management include the following:

- to speed up recovery from information-security incidents
- to reduce the costs and harm caused by information-security incidents
- to target investments that improve information security
- to improve the quality and productivity of registrar activity
- to optimise risk management economically and to prevent the materialisation of risks.

Identification and treatment of risks

Traficom does not impose an obligation to comply with any particular standard. Suitable frameworks include, for example, ISO/IEC 27005, NIST 800-30 and OCTAVE. Responsibility for risk management must be assigned, and risk-management activities must be scheduled. Risk assessments are typically carried out:

- on a regular annual basis
- when defining new services or functions
- following the materialisation of a possible risk.

2.3 Information assets

The registrar must operate a classification system for those information assets that are important for the registrar activity, together with an associated handling procedure. Up-to-date documentation of the classification criteria and the handling procedures must be drawn up.

2.3.1 Classification of information assets

The registrar must define a set of classification criteria appropriate to its own operations. An example of a classification:

- public
- confidential
- secret.

2.3.2 Information-asset documents

The documentation must address, among other things, rights of access and modification; storage and encryption; printing and copying; backup; receipt, sharing, sending and transport; and the archiving and destruction of assets.

2.4 Information-security monitoring

The registrar must continuously monitor its registrar activity. Monitoring makes it possible to detect, or to prevent entirely, situations that disrupt or threaten the activity.

2.4.1 Threat detection

Monitoring must take place through a management mechanism appropriate to the registrar activity, which detects problems affecting the state of information security as quickly as possible. Examples of situations that may be detected:

- denial-of-service attacks
- data leaks
- attempts at intrusion
- excessive access privileges.

2.4.2 Threat prevention

Monitoring mechanisms may include, for example:

- software alerts and service-quality indicators that flag deviations from normal operation
- notifications of detected hardware or software vulnerabilities, which give advance warning of information-security problems.

2.4.3 Documentation of monitoring

Up-to-date documentation of the monitoring mechanisms used in the registrar activity must be drawn up and maintained, so that the registrar is able, where necessary, to demonstrate the means by which it meets the requirements imposed on it.

2.5 Management of threats and incidents

The registrar must prepare clear procedural instructions in advance for dealing with situations that disrupt or threaten the information security of the registrar activity. These instructions serve to minimise the effects of such situations and to enable recovery from them without undue delay.

The procedural instructions must define:

- how information-security management is organised
- which actors are responsible for information security
- how the responsible persons can be reached.

The most important objective of the instructions is to put in place the capacity to identify the cause of an information-security problem as rapidly as possible and to minimise the consequences of the event. The instructions must also address special arrangements for remedial action in significant incident situations, such as on-call arrangements.

2.6 Change management

The registrar must organise changes, maintenance and updates so that they cause as little disruption to the registrar activity as possible.

The registrar must implement network, software, hardware, configuration, interface and equipment-room changes in a controlled and planned manner.

2.6.1 Planning of change work

In order to manage a change situation, the registrar must in advance:

- plan the progress of the change work
- calculate the resources required
- assess the effects and duration of the change work
- plan its follow-up actions in the event that the change work does not succeed as planned.

For example, when changing the software of equipment, it is advisable, where possible, to simulate the effects of the change in advance, so that any errors can be identified and corrected before the change is made.

2.6.2 Documentation of change work

The registrar must define and document in advance the processes and practices relating to change work, so that all change work is carried out in a planned and predictable manner.

2.7 Backups

The registrar must have a documented backup practice for information and systems critical to the registrar activity. In practice, the registrar should assess which information, systems and settings are necessary for the continuity of the registrar activity and ensure that they can be restored in an incident or crisis situation.

The backup practice should describe at least:

- which information and systems are backed up
- how often backups are taken
- how long backups are retained
- how backups are protected against unauthorised access, modification and destruction
- who is responsible for backups and restoration
- how and how often restoration is tested.

Backups must cover the information assets critical to the registrar's own operations, such as customer and contract data, information relating to the administration of domain names, system settings essential to the registrar activity, and any other information whose loss could prevent or materially disrupt the .fi domain name registrar activity.

The registrar must ensure that the level of protection applied to backups must correspond to the confidentiality and criticality of the data being backed up. The ability to restore must be tested regularly, because the mere existence of a backup does not in itself guarantee that the information can be restored when required.

2.8 Data protection in registrar activity

Registrars of .fi domain names collect and process the personal data of .fi domain name registrants for the purpose of registering .fi domain names. The processing of personal data is governed by the EU General Data Protection Regulation (679/2016, GDPR) and the national Data Protection Act (1050/2018). Section 170(1)(10) of the Act on Electronic Communications Services (917/2014) governs the disclosure of information.

As regards information entered in the domain name register, Traficom acts as the controller, and registrars act as processors of personal data on Traficom's behalf. When processing the personal data of domain name registrants in its registrar activity, the registrar must comply with the obligations imposed on processors by Article 28 of the GDPR.

However, the .fi domain name registrar acts as an independent controller within the meaning of the GDPR in respect of the personal data of .fi domain name registrants that it processes in its registrar activity and that are not required to be entered in the domain name register.

2.8.1 Personal data reported to the register

On the basis of the Act and the Regulation, the following personal data are collected about the registrant as part of registrar activity:

- name
- personal identity code or another unique identifier
- postal address
- telephone number
- e-mail address (service address).

> **⚠ Registrars established outside the EU/EEA**
>
> .fi domain name registrars established outside the EU/EEA may not register .fi domain names for private individuals unless there is a data-transfer arrangement accepted by the EU and currently in force with the country of establishment.
>
> This restriction also applies to registrars established in the United States that are not certified under the currently applicable data protection framework.

2.8.2 Purpose and duration of processing personal data

The registrar may process the personal data it has entered in the .fi domain name register only for as long as the .fi domain name is administered by that registrar and/or the domain name is in force, including any protection periods.

The registrar is responsible for deleting the personal data of .fi domain name registrants from its own systems when the legal basis for processing the data - the registrar's administration of the domain name - ends.

Where the registrar provides other services (for example website or e-mail services), the registrar must have some other GDPR-compliant basis for processing in relation to those services.

2.8.3 Rights of the domain name registrant

The registrant has the following rights:

- the right to know which parties process their personal data - the registrant's data is processed at least by the registrar and Traficom
- the right to know the purpose for which the data is used - the registration of the domain name, its maintenance and the resolution of disputes
- the right to verify their data and to have inaccurate data corrected
- the right to restrict the processing of personal data in the situations referred to in Article 18 of the GDPR
- the right to lodge a complaint with the Data Protection Ombudsman (tietosuoja.fi).

2.8.4 Resellers and subcontractors

Resellers act as processors of personal data on behalf of and for the account of the registrar. The registrar is responsible for ensuring that its resellers undertake to comply with the processor obligations under Article 28 of the GDPR. The registrar bears full responsibility for the conduct of its subcontractors.

2.9 Obligation to notify information-security incidents

The registrar must notify Traficom without delay if its domain name registrar activity is affected by a significant information-security breach, or by the threat of such a breach, or by another event that prevents or materially disrupts the activity.

Content of the notification

The notification must set out: the estimated duration of the incident or threat, its effects, the remedial measures taken, the measures taken to prevent recurrence and, where possible, the cause of the incident.

The notification is made primarily using the electronic form:

https://eservices.traficom.fi/ContactForms/form/tietoturvaloukkausilmoitus?langid=fi

In serious situations, or in order to investigate unauthorised changes, contact should also be made by telephone using the number notified to registrars.

2.9.1 Notification timetable

An incident notification must be made within 24 hours from the time the incident comes to the registrar's attention. If not all information is available, a preliminary notification is made within 24 hours and is supplemented at the latest three (3) days after the preliminary notification.

2.9.2 Significant information-security breaches

An incident may be regarded as significant where it affects:

- the registrar's own services and production systems
- the information security, personal data protection or trade secrets of the registrar's customers
- Traficom's administration of the Finnish .fi root zone (directly or indirectly).

An event may also be regarded as significant where it is frequently recurring, exceptionally long-lasting or apparently intentional, and if the incident cannot be resolved by the registrar's own measures alone.

Types of information-security breaches subject to the notification obligation

Significant information-security incidents that must be notified include, among others:

- intrusions into the registrar's information systems
- unauthorised access to the registrar's system
- a vulnerability or configuration error in the registrar's system that endangers information security
- login credentials coming into the possession of a third party
- credentials used for Traficom's systems coming into the possession of outside parties
- the possibility of unauthorised changes to the data of domain names administered by the registrar

- unauthorised changes to Traficom's domain name register by the registrar's own personnel
- denial-of-service attacks that paralyse the registrar's system or affect the operation of Traficom's system.

Traficom recommends that, at their discretion, registrars also notify information-security breaches and threats of breaches that are less than significant - such information may be relevant to Traficom's wider information-security duties.

2.10 Name servers

The registrar is responsible for ensuring that the name services linked to the .fi domain names provided to its customers are configured in accordance with the technical requirements.

A .fi domain name may be registered either with functioning name servers or without any name servers. Where name servers are provided, however, all of them must function. If the registrant wishes to keep the domain name registered in their name without functionality (a so-called parking service), the name servers must be removed from the .fi root.

Requirements for name servers

A domain name must be defined on at least two and at most ten name servers that are independent of one another (Traficom Regulation 68). Name servers are independent of one another where they operate:

- on different server hardware
- at different IP addresses
- behind different internet connections.

All name servers must in addition be reachable from the public internet, and their configuration must be verifiable by means of name-service queries carried out by Traficom.

Traficom regularly verifies the operation of all name servers. An e-mail notification is sent of any incorrect configurations either to the registrar or to the address indicated by the name-server administrator.

2.10.1 Recommendations

Traficom recommends that:

- the transfer of domain name data (AXFR/DNS zone transfer) be prevented from outside parties
- name servers should not disclose accurate software version information in response to version queries (to avoid information-security risks).

2.10.2 Requirements and recommendations for the SOA record

The MNAME field of the SOA (Start of Authority) record must contain the name of the primary name server. The RNAME field must contain a functioning e-mail address for the administrator (without the @ sign, which is replaced by a full stop, e.g. hostmaster.domain.fi).

Parameter	Recommended value	Explanation
Refresh	86400 (24 h)	How often secondary name servers check for changes
Retry	7200 (2 h)	Interval between retries after a failed query
Expire	3600000 (~1000 h)	How long the old zone file is retained
Minimum TTL	172800 (2 days)	Default lifetime for resource records
Serial number	YYYYMMDDnn	Date-based; increases with each update

The recommended format for the serial number is YYYYMMDDnn. The serial number must not be zero (0) and its value must increase by one with each update.

2.10.3 Name-service security extension DNSSEC

DNSSEC (Domain Name System Security Extensions) is a service that enhances the information security of the name service by enabling verification of the authenticity of origin and the integrity of the data obtained from a name server. DNSSEC can also be enabled for a .fi domain name.

Where DNSSEC is in use, responses to name-service queries are signed electronically, so that visitors to a website can be assured that they have been directed to the correct site.

DNSSEC deployment and DS records

The registrar may enable the DNSSEC service by signing the domain name data and adding DS records via the EPP interface or the browser interface.

Key rollover can be automated through the EPP interface.

The public keys for the .fi zone are published in the root zone. The trust anchor is available on IANA's DNSSEC pages (iana.org/dnssec).

More information: fi-domain-tech@traficom.fi

2.10.4 Name server test

Using the name server test available on Traficom's website, the registrar can check whether a .fi domain name has been configured in accordance with the requirements, whether the name services function correctly, and whether DNSSEC is in use. The test can also be used before registering a domain name and in connection with name-server changes.

Name server test

Zonemaster.fi checks the technical functioning of a domain name's name services and the correctness of its configuration. It tests, for example, delegation, name-server responses, DNSSEC, reachability and common configuration errors; it reports any shortcomings and warnings; and it provides recommendations for improving the name service.

More information: https://zonemaster.fi

2.11 Technical interfaces

As a technical interface to the .fi domain name register, the registrar uses either the browser interface or the EPP interface specified by Traficom.

2.11.1 Browser interface

The registrar may log in to Traficom's .fi domain name register via a browser interface. Logging in is two-stage: in addition to a username and password, a single-sign-on credential is required (an eight-digit one-time password delivered by text message). Logging in requires that the registrar has registered with Traficom.

2.11.2 EPP interface

EPP (Extensible Provisioning Protocol) is an XML-based technical interface to which the registrar can connect using its own client software. Traficom does not provide a ready-made client; the registrar must either develop one itself or procure one.

There is no obligation to deploy the EPP interface; it is also possible for the registrar to use both interfaces.

EPP interface address

Address: https://epp.domain.fi (port 700)

Before deployment, the client software must be tested in Traficom's EPP test environment.

The test documentation (EPP testing guidance, interface description, XML schemas) is available on Traficom's website.

Testing enquiries: fi-domain-tech@traficom.fi

2.11.3 RFC standards underlying EPP

RFC	Description
RFC 5730	Extensible Provisioning Protocol (EPP) - core protocol
RFC 5731	EPP Domain Name Mapping
RFC 5732	EPP Host Mapping
RFC 5733	EPP Contact Mapping
RFC 4310	DNS Security Extensions Mapping for EPP (earlier version)
RFC 5910	DNS Security Extensions Mapping for EPP (current version)

2.11.4 KATAKRI requirements when using the EPP interface

If the registrar uses Traficom's EPP interface, it must meet the requirements of sub-area I, technical information security, of the currently applicable version of Katakri, at security level IV, in respect of communications security and information-system security.

The Katakri requirements apply only to the domain name registrar activity. Where the registrar carries on other activities, the requirements do not apply to those activities. The current version of Katakri is available on the website of the Ministry of Defence (defmin.fi).

2.11.5 Other technical services

Traficom also offers the following technical services:

- Whois service: verification of the public data and availability of .fi domain names (whois.fi)
- DAS (Domain Availability Service): fast .fi domain name availability queries - das.domain.fi (port 715/UDP)
- OData interface: information on the domain names registered by organisations and entities, the name-server data and the contact details of administrators. The data is updated once per day. It does not include domain names reserved by private individuals (approximately 80 % coverage).
- RDAP (Registration Data Access Protocol) interface: a standardised query interface through which registry data on .fi domain names can be retrieved in structured JSON format.

Appendix A: Quick guide for new registrars - checklist

Work through the checklist below before registering as a .fi domain name registrar. All items must be completed before commencing the activity.

1. Statutory prerequisites

- ☐ I have familiarised myself with the Act on Electronic Communications Services (917/2014).
- ☐ I have familiarised myself with Traficom's Regulation 68/2014 M on domain names.
- ☐ My organisation has the capacity to meet the information-security obligations (administrative and technical information security).
- ☐ My organisation has the capacity to process customers' personal data in accordance with the GDPR.

2. Technical requirements

- ☐ The registrar's user account has been activated and logging in to the browser interface has been verified.
- ☐ If I wish to use the EPP interface: my client software has been successfully tested in Traficom's EPP test environment.
- ☐ If I use the EPP interface: I have satisfied the KATAKRI technical information-security requirements (communications security and information-system security, security level IV).
- ☐ I have at least two independent name servers in place (or I know how the name servers of my customers will be verified).

3. Administrative preparations

- ☐ I have drawn up an information-security policy or equivalent governance document.
- ☐ I have drawn up a description of the risk-management process.
- ☐ I have drawn up a classification system for information assets together with handling instructions.
- ☐ I have drawn up procedural instructions for incident situations (who is responsible and how they can be reached).
- ☐ I have drawn up a privacy notice.
- ☐ I have prepared guidance materials for customers on the form, content and lawfulness of domain names.
- ☐ I have defined the principles and procedures by which I ensure that only accurate and up-to-date details concerning my customers are held in the domain name register.
- ☐ My organisation has the capacity to identify its customers.

4. Registering with Traficom

- ☐ I have completed and returned the self-assessment tool specified by Traficom (the .fi domain name Cybermeter).
- ☐ I have completed Traficom's electronic registration form for registrars.

☐ I have notified, as my statutory service address, an e-mail address whose incoming messages I actively monitor.

☐ I have reserved sufficient funds in the prepayment account to cover domain name registrations.

☐ I have entered any resellers in the .fi domain name register.

Appendix B: Contact details

Below is a consolidated list of the important contact details and links referred to in this guide.

Finnish Transport and Communications Agency Traficom

Topic	Contact details
Information-security incident notifications (CERT)	**Information-security incident notification form; cert@traficom.fi**
EPP interface and technical enquiries	**fi-domain-tech@traficom.fi**
DNSSEC information	**fi-domain-tech@traficom.fi**
EPP interface	**https://epp.domain.fi (port 700)**
DAS service	**das.domain.fi (port 715/UDP)**
Whois service	**whois.fi**

Other authorities and registers

Authority or register	Web address
Finnish Patent and Registration Office (PRH) - Business Information System, Register of Associations, Trademark Register	**prh.fi**
European Union Intellectual Property Office (EUIPO) - EU Trademark Register	**euipo.europa.eu**
Office of the Data Protection Ombudsman (national supervisory authority)	**tietosuoja.fi**
IANA DNSSEC trust anchor	**iana.org/dnssec**
Current version of the Katakri audit tool	**defmin.fi**

Appendix C: Glossary

This appendix explains the key terms and abbreviations used in this guide.

ACE (ASCII Compatible Encoding) / Punycode

The technical representation used for internationalised domain names (IDN), in which national characters (such as ä, ö) are converted into an ASCII-compatible form. For example: ääkkönen.fi → xn--kknen-fraa0m.fi.

DAS (Domain Availability Service)

A Traficom service for quickly checking whether a .fi domain name is available for registration. The service operates at das.domain.fi on port 715/UDP. It does not return information about the holder of a domain name.

DNSSEC (Domain Name System Security Extensions)

A service that enhances the information security of the Domain Name System (DNS). DNSSEC enables the electronic signing of responses to name-service queries, by which the origin and integrity of the data can be verified. It mitigates, for example, DNS hijacking.

EPP (Extensible Provisioning Protocol)

An XML-based technical interface through which a domain name registrar can connect to the .fi domain name register using its own client software. Based on RFC standards 5730-5733. Requires compliance with KATAKRI requirements and successful testing in the EPP test environment.

EUIPO

European Union Intellectual Property Office. Maintains the EU Trademark Register. The registrar must provide its customers with a link to the EUIPO register before registering a domain name.

GDPR (General Data Protection Regulation)

The EU General Data Protection Regulation (679/2016). Governs the processing of personal data.

KATAKRI

The Finnish national security auditing criteria. Registrars using the EPP interface must meet the KATAKRI requirements for the technical information-security sub-area (I) at security level IV, in respect of communications security and information-system security. Current version: defmin.fi.

OData

A Traficom interface through which information on the domain names registered by organisations and entities, the name-server data and the contact details of administrators can be retrieved. The data is updated once per day. It does not include domain names reserved by private individuals (approximately 80 % coverage).

PRH (Finnish Patent and Registration Office)

A Finnish authority which maintains the Business Information System (YTJ), the Register of Associations and the Trademark Register. The registrar must provide its customers with links to PRH's public registers before registering a domain name.

Service address

The statutory e-mail address to which Traficom sends hearings and the service of documents. Messages sent to this address are deemed to have been served on the third day after dispatch. Notification of the service address is mandatory both for the registrar itself and for each customer's domain name.

RFC standard

Request for Comments - a series of documents describing technical standards and protocols of the internet. Traficom's EPP interface is based on RFC standards 5730-5733 (EPP) and 4310/5910 (DNSSEC mapping).

SOA record (Start of Authority)

A DNS record that defines the name-server settings for a domain name. It contains, among other things, the name of the primary name server (MNAME), the administrator's e-mail address (RNAME), the serial number and the timers (Refresh, Retry, Expire, TTL).

Traficom

The Finnish Transport and Communications Agency. The Finnish authority that administers the .fi country-code top-level domain, maintains the .fi domain name register and supervises the activities of domain name registrars. Acts as an independent controller in respect of the entire content of the .fi domain name register.

Registrar transfer key

A code by which the administration of a domain name is transferred from one domain name registrar to another. The former registrar generates the key in the domain name register system and delivers it to the new registrar or to the registrant. It must be delivered within five business days of a legitimate request.

Domain name transfer key

A code defined by Traficom by which a domain name is transferred from one registrant to another. The registrar sends the key to the current registrant of the domain name - the registrar does not itself see the content of the key code. The transfer must be carried out within five business days of the key being delivered.

Whois

A service for checking the public data of a .fi domain name and for confirming whether a particular domain name is available. Available at whois.fi. A Whois client program is required to use the service.